DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

SAIS-ZA

25 May 2021

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Cybersecurity Requirements for Teleworkers in the Vicinity of Smart Internet of Things (IoT) Applications and Devices

1. References:

a. H.R. 1668, Public Law 116-207, (IoT Cybersecurity Improvement Act of 2020), 2019–2020

b. Draft National Institute of Standards and Technology (NIST) Special Publication (SP) 800-213, (IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements), December 2020

c. Army Regulation 25-2, "Army Cybersecurity"

2. Purpose. This policy prescribes mandatory procedures for teleworkers to follow to mitigate data leakage of official government information; sets the conditions necessary for U.S. Army personnel to protect and safeguard DoD information and information systems; supports mission readiness and resiliency.

3. Background Information. See enclosure.

4. Policy. The Internet of Things (IoT) is the extension of internet connectivity into physical devices and everyday objects (reference a). Effective immediately, all personnel approved to telework must conduct work in an environment free of IoT devices. In the absence of this, teleworkers are required to remove all IoT devices with an automated listening function from their work area (e.g., smart TV, smart speaker, and other automated recording devices and networked devices). All personal mobile devices such as a smart phone or tablet, should either be turned off, removed from the immediate work area, or have the "audio" access function disabled from personal assistant applications (e.g., voice to text and automated assistants such as Siri).

5. Applicability. The provisions of this directive apply to all components of the Army, military, civilians, and contractors.

6. Point of Contact. Mr. Joseph, Chief, Policy and Risk Governance Division, Cybersecurity, Office of the CIO at (703) 545-1742 (DSN 865) or christopher.a.joseph4.civ@mail.mil.

7. Duration. This directive is rescinded on publication of revised regulation.

Encl

RAJ G. IYER
Chief Information Officer

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Futures Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Special Operations Command
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command

Superintendent, U.S. Military Academy
Director, U.S. Army Acquisition Support Center
Superintendent, Arlington National Cemetery
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
(CONT)

DISTRIBUTION: (CONT)

CF:
Under Secretary of Defense (Comptroller)/Chief Financial Officer of the
  Department of Defense
Under Secretary of Defense for Personnel and Readiness
Director, Defense Manpower Data Center
Director of Business Transformation
Commander, Eighth Army

BACKGROUND INFORMATION

1. Smart Internet of Things (IoT) devices – each embedded with sensors – are a network of items or applications ("things") that connect to the internet and emanate from a number of different technologies (reference a).

a. With the growth in the demand for smart home devices, average homes today, can have a variety of 70 or more different IoT listening or recording devices to include, but not limited to:

(1) Bluetooth wireless devices, speakers, mobile phone headsets, intercoms, hubs, home routers, printers, computers, laptops, tablets, mobile phones, smart watches, auto devices, gaming consoles, televisions (TVs), home entertainment centers, digital audio players, portable media, players, digital video recorders, webcams, cameras, sensors, fitness trackers, medical devices, weighing scales;

(2) smart home devices, kitchen appliances, washer and dryer machines, lights, home electric systems, smart energy management systems (e.g., thermostats, meters), smart security solutions (e.g., remote control digital door locks, doorbells, security cameras, alarms); and

(3) personal home assistant applications on mobile devices (e.g., Amazon's Echo wireless speaker with built-in Alexa application, Google's Assistant Home, Microsoft's Cortana, Apple's Siri, Samsung's Bixby, Bosch's Mykie, and others).

- Digital assistants can be 'awake and listening' even when users think they are not, listening all the time they powered on and recording transcripts of conversations. Background chatter is enough to trigger recordings which may happen inadvertently during conversations or by inadvertently pressing buttons on a voice assistant enabled device.

- Personal home assistants capture and record good or bad conversations and activities within a home.

b. The protocols of IoT devices are to collect a massive amount of information on daily activities and personal data to record information so that marketers can target audiences with intrusive digital advertisements.

c. The key risks that such devices represent are to confidentiality and privacy.

(1) Law enforcement can seek information from smart devices to solve crimes.

(2) Hackers and identity thieves can also access the service provider's compilation of data for their own benefits.

(3) Service providers such as Google and Amazon can provide audio clips and written transcripts of conversations and data searches to the public for marketing purposes or law enforcement purposes.

(4) Foreign intelligence services collect information from these devices for espionage or patterns of life

2. Despite their popularity and the benefits that IoT devices bring to the user, they also pose a significant security risk if not properly secured.

a. IoT devices allow remote access to physical and informational environments which can seek to target the cognitive attributes that influence decision making, the flow of information, and the interpretation of information by individuals or groups at any level within DoD.

b. IoT devices often lack the security functionality commonly present in conventional information technology (IT) equipment (e.g., computers, laptops).

c. Manufacturers do not always embed information security and privacy requirements into new products since technology moves at a rapid pace.

d. Most IoT devices have default usernames and passwords known to hackers.

e. A variety of IoT devices, that connect to the internet, provide numerous entry points or attack vectors for nefarious actors to exploit, which can then lead to exfiltration of data and compromise of confidentiality, integrity, and availability of DoD information systems.

(1) IoT devices have the ability to connect to information systems and can introduce unacceptable levels of risk to DoD and its information systems because most devices completely lack information system security controls and cybersecurity requirements in a manner that DoD expects.

(2) IoT devices can affect the security posture of DoD information systems and alter the information system's risk assessment that may then require the allocation of additional security controls or the introduction of compensating controls to reduce risk to acceptable levels.

(3) Many IoT devices maintain connections to cloud services and mobile, website applications that are central to the device's functionality that might store data – in the

device, the manufacturer's network, or a manufacturer contracted entity's network (e.g., cloud), etc.

(4) The architecture that supports IoT devices is increasingly global. IoT devices can connect to and transmit data to additional external systems and services, which a number of third parties across the globe provide and host.

(5) The power of all these devices can also combine into a botnet that can negatively impact the globe.

3. At a time when the majority of the workforce is remotely teleworking, IoT devices are an area of concern because it is likely that teleworkers use their personal devices, while connected to DoD's networks for official business conversations, in the vicinity of a smart device or application (e.g., Amazon's Alexa).

a. IoT devices and applications collect data (e.g., audio, video, or transcripts) to include data that requires a level of security and privacy such as critical unclassified information (CUI), personally identifiable information (PII), or DoD mission and operational data.

b. These practices pose privacy implications and serious data leakage, if teleworkers discuss details to DoD missions and operations in front of personal assistants and smart devices.

4. For these reasons, teleworkers must incorporate strong cyber hygiene practices in their daily telework routine.